Exhibit A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	22 Cr. 673 (LAK)
v.	:	
SAMUEL BANKMAN-FRIED,	:	
Defendant.	:	

DECLARATION OF DAVID SUN

David Sun declares pursuant to 28 U.S.C. § 1746 as follows:

1. I am over 18 years of age, of sound mind, and otherwise competent to make this Declaration. The evidence set out in the foregoing Declaration is based on my personal knowledge.

2. I have almost 30 years of professional experience in the fields of technology, computer networking, cybersecurity and computer forensics. I am currently an independent consultant specializing in computer forensics and cybersecurity. Prior to becoming an independent consultant, I was the Principal in charge of the cyber forensics and incident response practice at CliftonLarsonAllen (CLA), a Top 10 accounting firm. I came to that role through CLA's acquisition of my prior company SunBlock Systems, a consulting firm that specialized in cyber security, computer forensics and technology consulting where I was the Founder and Chief Executive Officer starting in 2002. I have personally conducted numerous computer forensic examinations and served as an expert for the private and public sectors, including a number of government agencies.

3. I was also the co-founder and Chief Technology Officer (CTO) of S34A, Inc., a company that performed advanced research in computer forensics for the Department of

Homeland Security and other government agencies. As CTO, I was responsible for the company's overall research efforts as we developed advanced computer forensics techniques and equipment for various United States government law enforcement agencies.

4. In addition, during the late 1990's, I was a Senior Network Engineer and Manager of Emerging Technology at UUNET/MCI, one of the first commercial Internet service providers (ISPs) that provided Tier 1 networking for much of the Internet during the dawn of the public Internet. Through my tenure at UUNET I became familiar with Virtual Private Networks (VPNs) as they were among the emerging technologies invented, refined and adopted for widespread use with the Internet during that time.

5. I am a Certified Information Systems Security Professional (CISSP) (arguably the most respected certification available for information systems security professionals), a Certified Computer Examiner (CCE), and an EnCase Certified Examiner (EnCE). I graduated from Virginia Polytechnic Institute and State University (aka Virginia Tech) with a Bachelor of Science and a Master of Science Degree in Electrical Engineering, and I have been an Adjunct Professor at George Mason University and a faculty member for the Virginia and Massachusetts State Bar's continuing education programs teaching courses on computer forensics and electronic evidence. I am regularly invited to speak at technical conferences and at government agencies on advancements in the field of computer forensics. I have been awarded multiple patents for inventions in the field of computer forensics, and I have authored numerous technical publications covering topics of interest in the fields of computer forensics, electromagnetics, and telecommunications.

6. I have testified as an expert witness or provided expert support in numerous litigation matters, including but not limited to matters involving digital data, computer forensics

and the various technologies and techniques used to obfuscate computer activity. I have also served as an expert or managed a team of experts involved in numerous complex matters involving data breaches, IT security, computer forensics and e-Discovery.

7. I submit this Declaration in support of the February 15, 2023 letter submission to the Court by counsel to Defendant Sam Bankman-Fried.

8. I have reviewed the Court's order dated February 1, 2023, indicating that Mr. Bankman-Fried may not "use any encrypted or ephemeral call or messaging application, including but not limited to Signal."[1] In addition, I reviewed various letters from the government discussing the need for this restriction and describing their concerns that applications such as Signal and Slack may encrypt their messages and be configured to autodelete messages after a short period of time, impeding the government's investigation.[2]

9. As an expert in technology with significant experience with Internet networking, VPNs and encrypted or ephemeral messaging applications, it is my opinion that messaging platforms (ephemeral or not) are technically and functionally different and unrelated to VPN technology.

I. Overview of Encrypted or Ephemeral Messaging Applications

10. Electronic messaging applications have existed for decades. AOL Instant Messenger is one of the early platforms gaining popularity in the 1990's. Over time users realized that these messages tended to linger and could be retrieved from either the sender's or recipient's device. Ephemeral messaging applications were created to allow people to send messages, knowing they will be deleted after a certain period of time. Snapchat is arguably the

[1] See February 1, 2023 Memorandum and Order, ECF No. 58.
[2] *See* January 27, 2023 Letter from United States Attorney Damian Williams to Honorable Lewis A. Kaplan, ECF No. 50; January 30, 2023 Letter from United States Attorney Damian Williams to Honorable Lewis A. Kaplan, ECF No. 53.

most well known of these applications. However, despite being deleted, these messages are still recoverable through forensic recovery techniques on the devices or through the eavesdropping of the message in transit (i.e., wiretapping). Encrypted messaging applications such as Signal make use of end-to-end encryption allowing only the sender and recipient the ability to decrypt the message if they provide a passcode. Messages intercepted in transit, even by the platform provider, are unintelligible as are messages forensically recovered from a device's memory storage. In short, this technology is designed for people to send messages to each other in a way that those intercepting them in transit or examining the sending or receiving devices, are unable to access the message without a decryption key (or password) provided by a user.

II. Overview of VPN Network Technology

11. VPN technology was created for and is generally used to extend a private network across a public network, such as the Internet. The most common use of VPNs is by corporations, government organizations and other large employers to securely allow a remote employee to access internal systems as if they were connected internally. In other words, they are designed to make the remote employee's computer appear to be inside a corporation's physical network (historically inside the company office) instead of their physical location. Encryption is deployed with VPN technology to keep the data from being susceptible to eavesdropping, much the same way that normal online credit transactions are also encrypted to protect credit card information.

12. Over the last decade, VPNs have been used in other ways as well. Consumer VPN Providers have emerged for personal use, serving as an intermediary between a user and a third-party such as a website or other online content provider. When used in this way, the VPN Provider establishes a "VPN tunnel" between a user and a third-party system. When using a

VPN Tunnel, data between the remote user and a third-party system flows through the VPN Provider's system. When data is tunneled, the IP address[3] for Internet traffic from the remote user is replaced by an IP address from the VPN Provider. This temporary IP address is assigned from the VPN Provider's allocation of IP addresses, and it is different from the remote user's true IP address. Because these temporary IP addresses are assigned to the VPN Provider, all internet traffic sent between the end user and a third-party appears as if it originated from the VPN Provider.

13. An analogy to how a VPN Tunnel operates is a PO Box at the post office. The user rents a PO Box from the postal service (equivalent to the VPN Provider). Instead of giving out his home address (computer IP address), the user provides the PO Box (VPN Provider's IP address). When a third party sends mail to the user (data from a third-party system) it goes to the PO Box for pickup or possible delivery by carrier to the user's home. From the Third Party's perspective, he only communicated with the PO Box (VPN Provider) and he cannot identify the user's home address (computer IP address).

III. VPN Tunnels Are Popular for Allowing Users to Change their Apparent Location

14. Computer traffic on the Internet does not contain any geographical information about the sender or recipient. Since this geographic information can be useful, many systems attempt to infer a user's geographic location based on the IP address of their user's computer. Similar to using the area code of a caller to infer where a person is calling from, the IP address of a computer can infer who the network provider is and where they serve the user.

15. However, in the same way that people can now request a number with any area code, assign it to a mobile phone travelling around the country and making the inference of a

[3] An IP address is the computer equivalent of a phone number. In order for a computer to communicate with other devices over the Internet, it must have a unique IP address.

caller's location from their area code inaccurate, users can use VPN Providers to create VPN Tunnels and change the location. In short, instead of making a remote employee's computer appear to be located inside the office building to enable secure data transfer, VPN technology is now commonly used to make a user's computer appear to be located in a location other than their home.

16. Using VPN Tunnels to change a user's apparent location may be used for various legitimate purposes. As an example, the Google search engine strives to provide highly relevant results. As part of that effort for relevance, they place significant weight on a user's location as a person in New York searching for "ice cream shop nearby" would not want to learn about ice cream shops in Paris, France. However, one can imagine how a VPN tunnel could be useful if you seek results relevant to a different geographic location (e.g., a listing of ice cream shops in Paris, France). Another popular example where people often use a VPN tunnel to change their location is with the Internet video streaming service Netflix which provides different titles based on a user's geographic location.

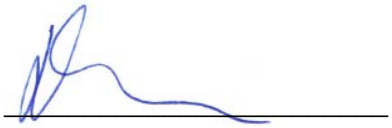
IV. Encrypted or Ephemeral Messaging Applications and VPNs are Very Different

17. As described above, encrypted or ephemeral messaging applications are designed to provide a method for passing messages privately between people using techniques such as encryption and autodeletion. VPNs, which do not have any autodeletion features, are a mechanism designed to emulate a computer being in a different location than their physical presence. While both technologies use encryption, their core uses are very different from a technology perspective, and a prohibition on using encrypted or ephemeral messaging or phone applications would not be regarded in the technology field as a prohibition on the use of VPNs.

The two technologies have substantially different functions and use cases and I consider any technical risks with using them to be different.

I declare under penalty of perjury that the foregoing is true and correct. Executed on February 15, 2023.

Dated: Great Falls, VA
February 15, 2023



David Sun